计算机研究与发展 DOI:10.7544/issn1000-1239.2016.20160684
Journal of Computer Research and Development 53(10):2137-2151,2016

大数据安全与隐私保护研究进展

曹珍富[1] 董晓蕾[1] 周 俊[1] 沈佳辰[1] 宁建廷[2] 巩俊卿[2]
[1](华东师范大学计算机科学与软件工程学院密码与网络安全系 上海 200062)
[2](上海交通大学计算机科学与工程系 上海 200240)
(zfcao@sei.ecnu.edu.cn)

Research Advances on Big Data Security and Privacy Preserving

Cao Zhenfu[1], Dong Xiaolei[1], Zhou Jun[1], Shen Jiachen[1], Ning Jianting[2], and Gong Junqing[2]
[1](*Department of Cryptography and Network Security, School of Computer Science and Software Engineering, East China Normal University, Shanghai* 200062)
[2](*Department of Computer Science and Engineering, Shanghai Jiao Tong University, Shanghai* 200240)

Abstract Nowadays, data security and privacy preserving have been definitely becoming one of the most crucial issues in the big data setting, where data encryption plays the most important role to achieve these goals. Therefore, to explore new data encryption techniques and new modes of big data processing has emerged as one of the most popular research topics all over the world. During the whole life cycle of data, the problems of computation, access control and data aggregation in the ciphertext domain (ciphertext computation, ciphertext access control and ciphertext data aggregation) are three critical issues in this research field. In this paper, we firstly review the state-of-the-art in the field of ciphertext computation, ciphertext access control and ciphertext data aggregation by identifying their inappropriateness. Based on it, a series of recent results in this research field are presented. In the aspect of ciphertext computation, a new method of designing efficient privacy preserving outsourced computation by reducing the usage times of public key encryption is proposed, with the implementation of a concrete construction which is realized by one time offline computation of any one-way trapdoor permutation without exploiting the technique of public key (fully) homomorphic encryption. In the aspect of ciphertext access control, a short ciphertext size traceable and revocable attribute-based encryption supporting flexible attributes is proposed. In the aspect of ciphertext data aggregation, an efficient privacy preserving data aggregation protocol with both input privacy and output privacy is devised without exploiting public key additive homomorphic encryption. Finally, we also suggest several interesting open research issues and the trend in the future.

Key words big data security; privacy preserving; ciphertext computation; ciphertext access control; ciphertext data aggregation

---

收稿日期:2016-06-15;**修回日期**:2016-09-20

基金项目:国家自然科学基金项目(61373154,61371083,61632012,61672239,61602180);高等学校博士学科点专项科研基金优先发展计划项目(20130073130004);上海市高科技项目(16511101400);上海市自然科学基金项目(16ZR1409200)
This work was supported by the National Natural Science Foundation of China (61373154, 61371083, 61632012, 61672239, 61602180), the Prioritized Development Projects Through the Specialized Research Fund for the Doctoral Program of Higher Education of China (20130073130004), Shanghai High-Tech Field Project (16511101400), and the Natural Science Foundation of Shanghai (16ZR1409200).

通信作者:董晓蕾(dongxiaolei@sei.ecnu.edu.cn)

摘 要 当前,用户数据的安全与隐私保护无疑成为大数据环境中最为重要的问题之一,而其最彻底的解决方式是通过加密所有数据来完成.因此,新的加密技术和在密文域上探索高效的大数据处理新模式是国内外当前的研究热点.在贯穿于整个数据生命周期中,密文域上的计算、访问控制和数据聚合(分别称为密文计算、密文访问控制和密文数据聚合)等问题已成为该领域的核心问题.主要针对密文计算、密文访问控制和密文数据聚合等当前国内外研究的现状进行综述,指出其存在的问题与不足.在此基础上,重点介绍了文章作者团队在大数据安全与隐私保护方面的最新研究成果.在密文计算方面,提出了通过减少公钥加密使用次数来设计高效的隐私保护外包计算的新方法,并设计了不依赖于公钥(全)同态加密,仅需一次离线计算任意单向陷门置换来实现安全外包计算的新方案.在密文访问控制方面,提出了支持大属性集合的、短密文的高效可追踪、可撤销属性基加密方案.在密文数据聚合方面,提出了不依赖于加法同态加密的、保护个体数据隐私且仅由授权接收方可成功解密聚合结果的高效隐私保护外包聚合方案.最后,还指出了该领域当前研究中需要解决的公开问题和未来的发展趋势.

关键词 大数据安全;隐私保护;密文计算;密文访问控制;密文数据聚合

中图法分类号 TP393

应用驱动的密码理论研究是我们团队长期以来的研究方向[1].基于各类应用问题的密码学新发展[2]和隐私保护[3]已出现了较为系统的研究成果,尤其是最近几年在面向大数据的应用驱动方面,新的安全理论问题也已被提出[4].

大数据(big data)指无法在可承受的时间范围内用常规软件工具进行捕捉、管理和处理的数据集合,是需要新处理模式才能具有更强的决策力、洞察发现力和流程优化能力的海量、高增长率和多样化的信息资产[5-6].用户的数据安全和隐私保护无疑是大数据背景下最为重要的问题之一[7].实现大数据安全与隐私保护的方法虽然种类多样,但其中最彻底的方法是通过加密来实现用户的数据安全和隐私保护.然而,随之而来的一个问题是:如何在密文域上实现类似于明文域上相同的大数据处理技术呢?这其中最重要的问题不仅仅是要解决诸如密文计算、密文访问控制和密文数据聚合等功能上的问题,更重要的问题是:要解决这些问题对应的新处理模式问题,即如同明文域上的大数据处理模式问题一样.

密文计算也称密态计算,是指在密文域上的计算以及符合访问权限的用户对密文域上的计算结果可进行确认并可获得对应的明文.为了保护用户数据的隐私,用户数据需要加密后存储,所以参与计算的密文数据一方面是由用户直接提供(用户需要的计算),另一方面通过密文搜索获得(运营商受托对某类数据作分析或统计计算).同态加密技术可以实现加密数据的处理,因此高效的同态加密算法在大数据外包中得到了广泛应用.同态加密(homomorphic encryption, HE)可分为单同态加密(single homomorphic encryption, SHE)和全同态加密(fully homomorphic encryption, FHE),前者是指该加密算法只满足加法同态或乘法同态之一,而后者指该加密算法同时满足加法同态和乘法同态.全同态加密实现了密文数据上同时进行加法与乘法运算的功能,从而能满足安全外包聚合与安全外包计算的功能需求.由于同态加密是公钥加密,其直接作用到数据上必然带来效率低下的问题,更不要说面向大数据的密文计算了.所以研究不依赖同态加密的密文计算是一个新的课题.

密文访问控制也称密态访问控制,是指对密文数据实现的访问控制.属性基加密(attribute-based encryption, ABE)通过对用户私钥设置属性集(或访问结构),为数据密文设置访问结构(或属性集),由属性集和访问结构之间的匹配关系确定其解密能力.特别是密文策略的属性基加密(ciphertext-policy attribute-based encryption, CP-ABE)是解决密文存储后访问控制问题的重要出发点.但仅具有“信道安全”的 CP-ABE 并不能真正解决密文访问控制问题,其主要原因是 CP-ABE 中不同密钥持有者能够解开同一份密文,且密钥持有者在泄露其密钥的情况下并不会招致任何损失.因此,对泄露密钥的用户实现可追踪是 CP-ABE 通往实际使用的必要步骤.与可追踪性紧密相关的性质便是可撤销性,即撤销泄露密钥或共享密钥的用户的解密能力.否则,即使系统具备的追踪机制能够帮助我们追踪到泄露密钥的用户,也并不能撤销非授权用户的解密能力,那么整个系统也是不完整的.

密文数据聚合也称密态数据聚合,是指在密文

域上实现数据分析与统计,即实现"单个数据、部分数据均不可知,但整体数据可知"功能.为了完成数据分析或统计,各部门通常是委托运营商(第三方)来实现,而运营商可能是半可信的甚至是恶意的(比如被收买):半可信的是指运营商严格执行协议的规定,但通过与用户的交互最大程度地提取有关用户隐私的秘密信息;恶意的是指运营商可以任意破坏协议的执行来获得用户隐私的秘密信息.密文数据聚合正是因解决这方面问题而提出的前沿课题,它能够实现在完成数据分析或统计的过程中保证用户的个人数据隐私.这方面目前大部分工作都是使用公钥单同态加密和密钥预分配来实现,效率不高、可用性差.

国内外针对密文计算、密文访问控制和密文数据聚合等已有的研究思路绝大部分都是分别通过全同态加密、属性基加密和单同态加密来实现.但这些加密全部是公钥加密,它们或因计算开销大,或因无法抵抗密钥共享攻击而对普通数据都显得"力不从心",因而也更无法直接应用在大数据环境中,以高效地解决大数据安全与隐私保护问题.换言之,密文域上的大数据系统尤其需要新的处理模式,即通过尽量减少公钥加密使用次数(最优时一次)的方法,且不依赖(全)同态加密,来设计高效的密文计算、密文访问控制和密文数据聚合方案.

本文在分析了密文计算、密文访问控制和密文数据聚合等国内外研究现状的基础上,指出了传统的使用公钥全同态加密、"信道安全"属性基加密和单同态加密来分别实现密文计算、密文访问控制和密文数据聚合的不足,同时给出了适应于大数据系统安全与隐私保护需求的新型的处理模式.最后,本文还给出了这方面存在的问题与未来的研究方向.

1 密文计算

1.1 基于全同态加密的密文计算

当前的密文计算主要是基于公钥全同态加密实现.其一般方法如图1所示.

首先,各用户即数据发送方利用公钥全同态加密算法加密每一个输入数据 $x_i(i=1,2,\cdots,n)$;然后,云服务器可以在密文域上进行函数 F 运算,并将同样是在密文域上的计算结果返回给接收方;最后,授权的数据接收方可以利用公钥全同态加密的私钥成功解密,得到明文域上的函数 F 计算结果.在利用传统的基于公钥全同态加密技术[8-30]实现密文计算时,需要将计算开销本来就较大的公钥全同态

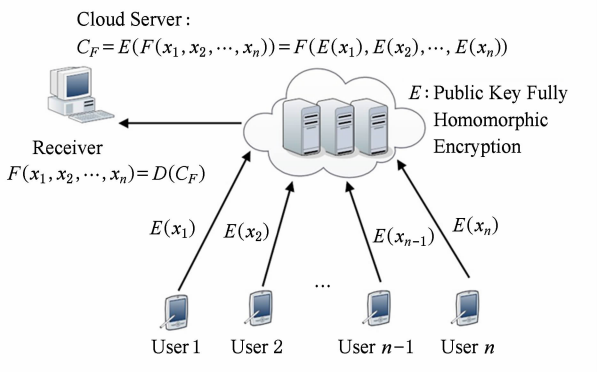


Fig. 1 Ciphertext computation based on public key fully homomorphic encryption.

图1 基于公钥全同态加密的密文计算

加密作用在每一个输入数据上来实现隐私保护,无法满足大数据环境中资源受限的移动终端设备在性能上的客观需求,且违背混合加密体制中用公钥加密来加密较短的对称密钥、用对称密钥来加密数据的基本原则.1978年由Rivest,Shamir和Adleman[31]提出了同态加密的概念,同年他们[32]提出了RSA公钥加密算法具有乘法同态性(单同态),该方案的安全性基于大整数分解.第1个基于离散对数问题的公钥加密体制ElGamal[33]具有第2项密文的乘法同态性(部分单同态).Goldwasser和Micali[34]提出了一种满足加法同态的加密方案,其安全性基于二次剩余假设,由Benaloh[35]给出的改进版本也具有加法同态性.Naccach等人[36]、Okamoto等人[37]和Paillier[38]分别提出了实现多次加法同态运算的加密方案.2005年,第1种同时支持任意多次加法同态运算和一次乘法同态运算的方案由Boneh等人[39]提出,该方案是距离全同态加密方案最近的一项工作.

2009年,Gentry[40]提出了基于理想格的全同态构造方法,这是第1个语义安全的全同态加密方案.它在理论上无懈可击,但实现起来却颇有难度.2010年,Smart和Vercauteren[41]对Gentry方案进行了第1次实现.2010年,Stehle与Steinfeld[42]提出了另一种对Gentry方案的实现,通过引入解密误差的方法来缩短计算次数.2011年,Gentry和Halevi[43]采用类似于Smart和Vercauteren的方法来实现,在生成密钥时去掉了行列式为素数这个条件,提出了4种不同规模环境下的参数.2010年,Dijk等人[44]提出了基于整数环上运算的类同态方案,并且使用Gentry的构造方法将其转化为全同态方案.总体而言,由于Gentry方案在构造上的局限性,使其实现效率很低,因此并不实用.

为促成同态密码在实际中的应用,除了采取各种技巧来提高效率之外,在方案的构造阶段,还存在另一种思路,就是针对实际应用的特点,降低对加密算法的要求,利用效率较高的类同态加密方案来满足实际需要[8-30,45-49]. 自从 LWE(learning with error)问题[8]被提出以来,它就被应用于密码体制的构建中. Halvei 等人[9]在 2010 年基于 BGN 密码提出了一种实用的方案,其安全性基于 ring-LWE 问题,支持任意次数的加法和一次乘法,支持较大的消息空间,是一个高效而实用的方案. 但是,只能计算一次乘法运算的性质仍然限制了其应用范围. 2011 年,Brakerski 和 Vaikuntanathan[10]使用 Gentry 的构造方法和重线性化技术的基本原理,分别基于 ring-LWE 困难问题和标准 LWE 困难问题构造了 2 个全同态加密方案. 其他密码学家们[11-15]也在积极尝试对 Gentry 的构造方法进行改进,并且提出了一系列基于 LWE 的同态加密方案.

全同态加密实现了密文数据上同时进行加法与乘法运算的功能,从而能满足安全外包计算的功能需求. 但是,Lauter 等[16]指出:目前的全同态加密技术的计算代价仍然无法达到真实应用的需求.

在大数据外包计算的可验证性方面,Gennaro 等人[17]形式化地定义了可验证计算方案,并在 Yao 的混淆电路[18]的基础上构造了一个非交互的可验证计算方案. Chung 等人[19]在 FHE 的基础上构造了非交互的可验证计算方案,该方案的优势在于其公钥长度较短. Applebaum 等人[20]利用消息认证码提出了一种更加简单高效的构造可验证计算的方法. Benabbas 等人[21]则针对某些特殊函数构造了高效的可验证计算方案. Barbosa 等人[22]以模块化的方式,利用全同态加密技术、函数加密技术和消息认证码技术提出了一个可验证的函数加密方案与可代理的同态加密方案. Fiore 等人[23]则基于同态 HASH 函数、针对加密数据给出了高效的可验证计算方案.

Parno 等人[24]首次提出了可公开验证计算的概念,并基于密钥策略的属性基加密方案(KP-ABE)构造了可公开验证计算方案. Fiore 等人[25]在 Benabbas 等人[22]所构造方案的基础上,构造了针对高阶多项式函数和矩阵乘积的支持公开验证的方案. Catalano 等人[26]通过引入代数单向函数来构造针对高阶多项式与矩阵乘积的支持公开验证的方案. Papamanthou 等人[27]构造了云环境下可验证签名的动态计算的新模型.

Choi 等人[28]给出了支持多客户端、非交互的可验证计算的构造. Goldwasser 等人在文献[29]中给出了多输入的函数加密的构造,并在此基础之上,对如何将其应用于多客户端可验证计算方案的构造作了讨论. Gordon 等人[30]给出了多客户端的可验证计算中更强的安全性和隐私性模型的探讨,并分别基于属性基加密、全同态加密以及 Yao 的混淆电路构造了支持多客户端的可验证计算方案.

1.2 不依赖于全同态加密的密文计算

毋庸置疑,当今信息安全发展的另一大趋势是大数据技术,其特点可以概括为:理想状况下很有效,但在有敌手的状况下无效[50]. 因为敌手可以任意篡改外包存储的数据,使得随之得到的计算统计分析结果出错,误导决策,严重地影响人们的生产生活. 目前针对上述问题,主要有 2 种解决方案:1)UC 通用组合技术,即证明设计的大数据方案在现实环境下和理想环境下不可区分;2)密文大数据技术,其中最重要的是实现密文域上的安全外包计算. 然而,基于公钥全同态加密的密文计算是否能够真正解决密文域上的大数据处理问题呢? 答案是否定的[50]. 国内外有关可验证外包计算的研究工作[8-30,45-49,51-58]多基于公钥全同态加密技术实现,其巨大的计算开销无法满足面向大数据系统的性能需求. 更重要的是,直接将公钥全同态加密应用于数据本身,违背了混合加密体制中用公钥加密算法来加密较短的对称密钥,用对称密钥来加密大数据这一基本原则. 文献[45-49]试图通过减少公钥全同态加密本身的计算开销来构造轻量化的密文计算方案,然而其结果仍无法满足大数据背景下的客观需求. 因此,我们团队开创性地提出了在不得不使用公钥加密实现隐私保护前提下,通过减少公钥加密的使用次数(最低一次)来实现不依赖公钥全同态加密的、高效的隐私保护外包计算新理论、新方法[50,59]. 在利用传统的利用公钥全同态加密技术[8-30]实现密文计算时,需要将计算开销本来就较大的公钥全同态加密作用在每一个输入数据上来实现隐私保护,无法满足大数据环境中资源受限的移动终端设备在性能上的客观需求;而我们团队提出的不依赖于公钥全同态加密的密文计算新方法,仅需离线状态下一次任意单向陷门置换运算,在线状态时仅需要简单的加法、乘法运算即能达到对 n 个数据的隐私保护. 其主要实现思路如图 2 所示.

1) 离线阶段,用任意单向陷门置换或公钥加密函数加密随机数,用作对称密钥分发;

2) 在线阶段,用生成的对称密钥利用简单的加

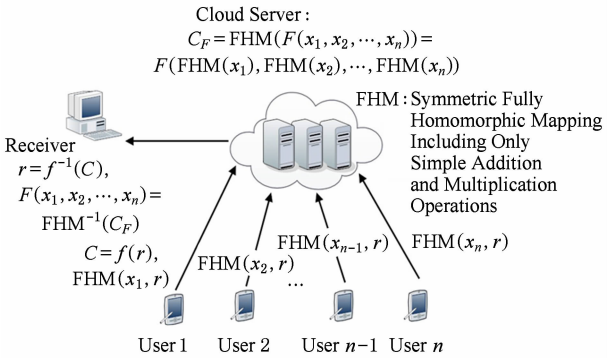


Fig. 2 Ciphertext computation without public key fully homomorphic encryption.

图 2 不依赖于公钥全同态加密的密文计算

法或乘法运算对数据本身通过对称的全同态映射 FHM 进行加密;

3) 存储与计算资源充足的云服务器在密文域上计算函数;

4) 授权用户可先用公钥加密算法对应的私钥求解单向陷门置换的逆得到对称密钥,然后用对称密钥解密密文计算结果并验证其正确性.

同时,我们团队还利用上述不依赖于公钥全同态加密的隐私保护密文计算新方法提出了不依赖于公钥全同态加密的可验证外包计算技术[60],使得计算资源受限的移动设备将以 $x_1,x_2,\cdots,x_n$ 为输入的函数 F 外包给计算资源充足的云服务器完成. 现有工作主要依赖于重客户端的 Yao 的乱码电路和全同态加密技术. 我们基于任意单向陷门置换提出了一个高效的可验证外包计算方案 EVOC[60]. 解决了 Gennaro 等人提出的"如何设计一个不依赖于全同态加密的高效可验证外包计算"这一挑战性公开问题. 最后,形式化安全性证明和仿真实验表明了所构造方案 EVOC 能满足可验证外包计算的安全与隐私保护需求,并与现有工作相比具有较低的计算与通信开销.

此外,我们团队还利用不依赖于公钥全同态加密的隐私保护密文计算新方法高效地解决了能同时保护文本隐私与模板隐私的安全外包模式匹配问题[61];并在电子医疗云计算系统中,提出了高效的隐私保护医疗图像特征提取与匹配协议,构建了智慧诊疗系统[62]. 电子医疗系统越来越广泛地通过医疗数据挖掘和医疗图像特征提取等方式,应用于人类健康管理、病情建模、早期干预和基于证据的医疗诊断. 由于可穿戴设备资源受限,要求将频繁采集的个人健康信息(personal health information, PHI)外包存储或外包计算到云服务器端,却随之带来一系列安全与隐私保护问题. 现有工作多集中于静态密文医疗数据的访问控制与分析,未对动态密文健康状态波动信息与密文医疗图像作出相关研究. 我们在基于云的电子医疗系统中,提出了一个高效的隐私保护动态医疗文本挖掘与图像特征提取方案 PPDM:病兆函数相关性匹配方案 PPDM1 以及能同时保护病人病历图像隐私与医生病兆模板隐私的医疗图像特征提取与匹配方案 PPDM2,为实现隐私保护的智能诊疗专家系统提供了有利保障. 最后,形式化安全性证明和仿真实验表明,与现有方案相比,所构造方案 PPDM 具有更高的安全性(输入隐私的无条件安全和输出隐私的 CCA2 安全)和在计算、通信开销方面的优势.

1.3 存在问题与未来研究方向

本节主要回顾了在密文计算研究领域的国内外研究现状,指明了基于公钥全同态加密算法实现的密文计算协议的缺陷与不足;并在此基础上重点介绍了不依赖于公钥全同态加密、仅需一次离线任意单向陷门置换实现的密文计算新方法. 然而,现有工作多在随机预言机模型下构造,且对外包密文计算结果的可验证性尚未作出深入研究. 由于在恶意模型下,云服务器可通过任意行为来破坏协议的执行,即有动机通过返回任意计算结果对资源受限的移动用户进行欺诈. 设计标准模型下或通用组合安全模型下的高效可验证密文计算协议是进一步的研究方向.

2 密文访问控制

2.1 "信道安全"属性基加密

密文访问控制可以但不能完全基于传统的属性基加密实现[50],传统的属性基加密方案仅考虑信道安全,即选择明文安全(chosen plaintext attack, CPA)或适应性选择密文安全(adaptive chosen ciphertext attack, CCA2). Sahai 和 Waters[63] 在 2005 年提出模糊身份加密方案的时候,只实现了最简单的访问表达能力——仅要求身份的交集达到给定的阈值,即将身份的匹配关系由原来的"完全匹配"变为"相似匹配",允许存在一些小的误差. Cheung 和 Newport[64] 在标准模型和标准假设(BDBH 假设)下给出了一个可证明安全的方案,但是访问结构只能支持与门. 文献[64]以访问策略的表达能力(只支持一个 AND 关系)为代价、文献[65]以部分表达能力(有界的访问策略)和部分性能(较大的密文长度)为代价来设计

可证明安全的 CP-ABE. Emura 等人[66]给出了一个常量密文的密文策略属性基加密系统,但该系统的访问策略只能支持单一的 AND 关系. Herranz 等人[67]则在访问策略的表达能力方面前进了一步,给出了能够支持门限策略的常量密文策略属性基加密系统. Lewko 等人[68]和 Okamoto 等人[69]分别给出了属性个数完全不受限制的属性基加密方案,但这 2 个方案的效率不高且证明相对复杂. 在 2013 年, Rouselakis 和 Waters[70]给出了支持大属性集合的 ABE 方案,并利用"编程和消去"(program and cancel)证明技术和"q 类"(q-type)困难问题假设证明其方案为选择性安全. Green 等人[71]结合云计算模型,允许用户提供给云服务器一个转换密钥,允许云服务器转换成满足用户属性的 ElGamal 型密文;而云服务器在此过程中并不能读取用户的明文. 2012 年, Lewko 等人[72]首次在适应性模型下给出了支持属性在访问结构中重复出现任意多次的属性基加密方案. 2013 年, Hohenberger 和 Waters[73]通过双线性群上的数学性质,将一些经典的属性基加密方案中的解密所需双线性运算次数都减小为常数. 考虑到属性基加密在资源受限移动设备上的应用, Hohenberger 等人[74]在 2014 年提出了高效的在线离线属性基加密方案. Boneh 等人[75]在 2014 年给出了基于格和全密钥同态加密(fully key-homomorphic encryption)的具有短密钥的(密钥策略)属性基加密系统. Yamada 等人[76]在 2014 年给出了支持任意个属性集合和访问结构的紧凑参数(compact parameters)的非单调的 CP-ABE. 短密文属性基密码的构造,往往会导致弱的安全性——选择安全性或者需要参数化的假设.

Kowalczyk 和 Lewko[77]结合在双系统模型下在 DLIN 假设下给出了完全安全的短公开参数的 KP-ABE. Chen 等人[78]基于改进的双系统模型给出了更为高效的素数阶的属性基加密方案,方案的运行效率较现方案有 25%～50%不同程度的提升. Gorbunov 和 Vinayagamurthy[79]基于标准的 LWE 问题给出了支持 branching programs 的短密文 ABE. Attrapadung 等人[80]研究了 ABE 与其他功能加密之间的相互转化关系,并给出了首个非单调的支持大属性集合的常数密文 CP-ABE、首个密钥长度为常数的 KP-ABE、首个支持 arithmetic span programs 的常数密文 ABE. Brakerski 等人[81]基于 LWE 难题给出了首个支持大属性集合的 KP-ABE. 在属性基加密完全安全性所依赖的双系统技术的素数阶实现方面,我们团队[82]采用双系统群模拟法(dual system group method)给出了一个嵌套双系统证明技术的更加高效灵活的素数阶实现. 该项工作的最终效果是一个更加高效且具备灵活参数调节机制的非受限层次身份基加密(UHIBE). 最近,我们团队[83]与 Attrapadung 等人[84]独立地给出了第 1 个采用素数阶双线性群实现的在多挑战模型下紧规约安全的身份基加密系统,该项工作已经发表在公钥密码学顶级会议 PKC 2016 上. 这 2 项工作均是双系统群方法(向量空间模拟技术之一)在复杂情形下的扩展和应用.

2.2 "信道安全+"属性基加密

自香农在 1948 年提出经典信道通信模型以来,历经几十年的发展历程,直到 Diffie-Hellman 密钥交换的出现,以至当前如火如荼的建立在选择明文安全或适应性选择密文安全模型基础上的属性基加密,国内外学者一直沿袭着信道安全模型的脚步开展了一系列重要研究并取得了里程碑式的结果[65-122]. 然而,基于信道安全模型、仅考虑传输过程中安全问题的属性基加密是否能够真正解决密文数据的访问控制问题呢? 答案是否定的[50]. 让我们通过加密电视机顶盒的例子来阐明我们的观点. 首先,加密电视的授权用户可能会出卖或出租自己的解密密钥给其他人,而不影响自己的解密,通过相互间的密钥共享,使得该集体能解密并观看更多的电视频道,以达到"双赢"乃至"多赢"的结果. 为了解决此类"慷集体之慨,谋私人之利"的安全问题,有效抵抗密钥共享攻击,必须从应用需求出发考虑可追踪的安全模型,对密钥泄露源进行有效追踪. 其次,授权用户还可能会出卖或出租自己的解密密钥用来复制机顶盒设备,因此,如何消除市面上大量复制的该设备就必须考虑可撤销的安全模型. 在传统信道安全模型的基础上,融合可追踪、可撤销的安全模型,从而迈入"信道安全+"的时代,成为了当今信息安全发展的一大趋势.

可追踪、可撤销属性基加密主要思想如图 3 所示. 白盒可追踪是指私钥泄露方直接出售解密密钥,而黑盒可追踪是指解密密钥和解密算法被隐藏在黑盒中. 可追踪、可撤销属性基加密不仅要求对私钥泄漏源,即图 3 白盒可追踪属性基加密的用户 S_C 和黑盒可追踪属性基加密的用户 S_A 实现有效追溯,还要求对私钥泄漏用户 S_C, S_A 以及非法获得密文访问控制权限的非授权用户的访问控制能力进行及时撤销.

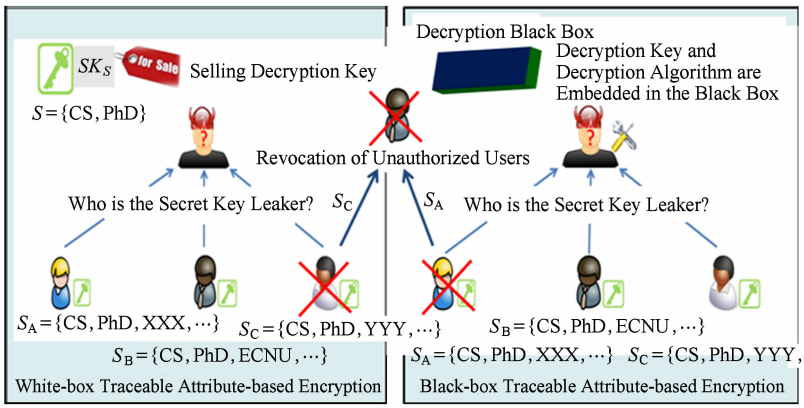


Fig. 3 Traceable and revocable attribute-based encryption.

图 3 可追踪可撤销属性基加密

在可追踪方面,2008 年,Jason 等人[85]提出了第 1 个密钥可追踪选择性安全的系统,但他们的系统是基于一个可信第三方机构的,解密者每次解密都要与这个第三方机构进行交互,这个第三方机构会成为系统的性能瓶颈. 2009 年,Yu 等人[86]给出了一个可追踪的密钥策略属性基加密方案,该方案在密钥关联的访问策略中嵌入身份信息的每一位信息,每一位信息作为一个属性嵌入在访问策略中. 2011 年,Katz 和 Schroder[87]提出了谓词加密中的可追踪性概念,并给出了可追踪的内积谓词加密系统,其所付出的代价与系统中的用户数量呈线性关系. 2013 年,我们团队[88]给出了第 1 个同时支持高表达力和白盒可追踪的密文策略属性基加密系统,实现了对泄露密钥的恶意用户的白盒可追踪. 该方案达到了标准模型下的适应性安全,允许任意单调访问结构作为访问策略,其密文大小的密文的访问策略大小成线性关系. 但该方案需要维护一个记录用户的列表来实现白盒可追踪,当用户数量逐渐变大后对用户列表的维护,会成为该方案实际应用当中的一个瓶颈. 同年,我们团队[90]又提出了第 1 个同时支持高表达力和抗全合谋黑盒可追踪性的密文策略属性基加密系统. 作为一个具有抗全合谋的黑盒可追踪的属性基加密系统来说,所提方案的密文大小达到了目前所知的最好水平(与系统的用户总数成亚线性关系). 随后,我们团队[91-92]提出了第 1 个切实可行的同时支持白盒可追踪和大属性空间的构造(公开参数大小与属性空间大小无关)的密文策略属性基加密系统,该方案无需维护一个记录用户的列表,而仅需在系统初始化时记录一小部分预先设定的参数即可,从而使得属性基加密系统从理论向实际应用又向前迈进了一步. 最近,我们团队[89,93]还给出了支持高表达力、白盒可追踪、可追责和公开审计的密文策略属性基加密与更短密文、抗全合谋、抗适应性类密钥和固定策略解密黑盒的高效黑盒可追踪密文策略属性基加密.

在可撤销方面,文献[94]给出了一个解决方法,是通过给每个用户颁发一个额外的终止日期的属性来限制密钥的使用时间. 之后,也有一些工作考虑了属性基加密系统中的密钥撤销问题,但其所采用的更新方式都不能满足实际应用需求. 在更新(或者撤销)密钥时,密钥更新机构的工作量与系统中用户数量成线性相关关系,而且每个用户还需与密钥更新机构之间保持一个安全信道. 另一方面,虽然目前已经有一些结合实际应用(如云计算、无线传感网等)的属性基加密系统相关的撤销方案被提出来,但这些方案中都是把用户作为最小单位进行撤销的,还是延续了身份基加密的撤销机制,没有充分体现出属性基加密的灵活性,即每次撤销一个用户,而不是在撤销一个用户的某些属性的同时允许用户的其他的有效属性仍然可以用来解密. 事实上,我们团队[95]在 2009 年就提出了第 1 个多用单向的属性基代理重加密方案,基于授权有效地实现了由一个访问控制结构到另一任意访问控制结构的完全密钥撤销. 之后,我们团队[96]提出了(无需授权的)可撤销属性基加密方案,引起 Sahai 等人[97]的兴趣,他们在 2012 年的美密会上提出了另一个可撤销属性基加密方案. 该方案同样采用二叉树思想,将每个用户设置为与二叉树的叶节点相关,使得密钥更新数量与用户数量呈对数关系,同时结合了“密文代理”的性质,以达到高效的密钥撤销. 此外,我们团队[123]提出了第 1 个基于属性的代理重加密方案;我们团队[124]在 ESORICS 2011 首次提出无中央机构的门限多机构

的属性加密方案;我们团队[125]设计了可同时满足白盒可追踪、可撤销性质的多机构属性基加密方案,并利用该构造在电子医疗云计算系统中实现了多级隐私保护.

从当前国内外的研究现状来看,虽然当前属性基加密在表达能力、通信效率、计算效率以及"信道安全+(可追踪/可撤销)"等方面受到了学术界广泛的研究,并越来越靠近实际应用,但距离面向大数据系统的实际应用还有一定的距离.

2.3 存在问题与未来研究方向

本节主要回顾了基于信道安全属性基加密实现密文访问控制的国内外最新研究进展,并指出了仅满足信道安全(选择明文攻击、适应性选择密文攻击)并不能满足从应用出发的密文访问控制的安全性需求.并在此基础上重点介绍了"信道安全+"新安全模型与同时满足可追踪、可撤销、多机构性质的属性基加密方案的构造与设计.为了适应大数据背景下计算、通信能力受限的移动用户的性能需求,寻求更短密文、短密钥、短公开参数的,且具备丰富表达能力的,基于简单标准难题假设的可追踪、可撤销、多机构属性基加密方案是一个值得进一步研究的方向.

3 密文数据聚合

3.1 基于同态加密的密文数据聚合

在密文数据聚合方面,国内外最新的研究工作多基于公钥加法同态加密(如 Paillier 加密算法)实现,其主要思想如图 4 所示:

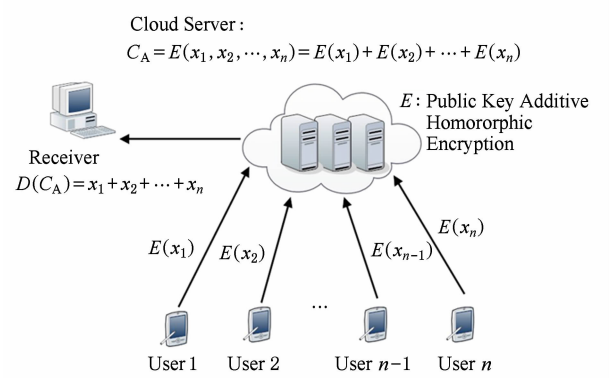


Fig. 4 Ciphertext data aggregation based on homomorphic encryption.

图 4 基于同态加密的密文数据聚合

首先,利用公钥加法同态加密对每一个个体数据加密以实现个体数据的隐私保护;同时,云服务器可利用公钥同态加密算法的加法同态性在密文域上进行数据聚合及各种丰富类型的统计与分析;最后,拥有公钥同态加密算法对应私钥的授权用户可解密聚合运算的结果.在运用上述密文聚合协议实现隐私保护方面有一系列研究进展[107-115].2012 年 Zhang 等人[107]提出了一套细粒度的隐私保护配对协议,使得 2 个用户在各自文档描述不被泄露的前提下,与其具有相似文档描述的用户实现成功匹配.2013 年 Liang 等人[108]在移动社交网络中研究隐私保护的用户匹配,并提出了一系列的用户文档描述匹配协议.另一方面,隐私保护的群分级也是一个有意义的研究问题.2012 年 Li 等人[109]提出了一个隐私保护的多方排序协议,保证只要在最终排序结果隐藏的情况下,敌手无法将用户的身份与其对应的文档描述进行有效联系.2013 年 Zhang 等人[110]提出了一个可验证的隐私保护分类分级协议,且在同年 Li 等人[111]提出了一个隐私保护的位置查询协议.然而,上述协议均依赖于公钥同态加密技术来实现隐私保护,计算开销巨大.

国内外大量的研究工作致力于智能电网中隐私保护的数据聚合与动态计费问题.2012 年 Lu 等人[112]在智能电网通信中提出了一个隐私保护的数据聚合方案 EPPA.该方案利用超递增向量和 Paillier 同态加密技术对多维数据进行密文聚合.但是,为验证 n 个加密用电量,即使在采用批量验证技术的前提下,仍需要进行 $n+1$ 次配对运算和 $n-1$ 次模乘运算.因此,该方案的计算复杂度随用户数量与用电量采集频率的增加迅速递增,不能满足智能电网中设计轻量的隐私保护数据聚合协议的基本要求.同年,Erkin 等人[113]利用 Paillier 同态加密技术提出了一个基于时间和空间特性的、隐私保护用电数据聚合方案.2013 年 Liang 等人[114]提出了一个智能电网中基于实时用电量的、隐私保护的动态计费方案.该方案在利用全同态加密技术保护用户实时用电量隐私的前提下,以用户个人用电量与用户所在地区用电量为标准来实现动态峰谷计费.2014 年 Won 等人[115]在智能电网中提出了一个能够有效保护差分隐私,高效容侵的智能传感数据聚合协议.然而,上述国内外现有工作均利用公钥同态加密技术作用于每一个实时用电数据,以实现隐私保护的数据聚合,既不符合混合加密体制的基本原则,且计算开销大,不适于存储、计算及通信资源受限的智能电表.

3.2 不基于同态加密的密文数据聚合

如何在面向大数据系统的资源非对称分布的环

境下设计安全高效且隐私保护的外包数据聚合与分析协议是近年来国内外学者研究的焦点.最近,我们团队[59]在国际上首次考虑避开全同态公钥加密和零知识证明技术,利用任意单向陷门置换提出高效的基于单用户时间序列隐私保护数据聚合方案,仅需离线执行一次任意单向陷门置换及其求逆运算便能实现对多个数据的隐私保护聚合[2-3,50].其主要思想如图5所示:

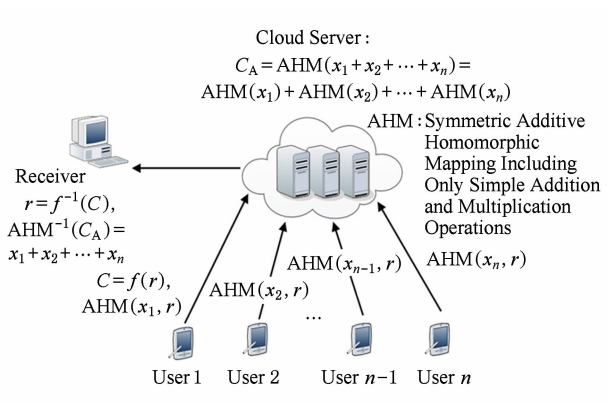


Fig. 5 Ciphertext data aggregation without homomorphic encryption.

图5 不基于同态加密的密文数据聚合

首先,在离线状态下利用一次任意单向陷门置换 f 加密随机数 r,用于对称密钥分发,在线状态利用对称密钥 r 通过仅包含加法和乘法等简单运算的对称加法同态映射 AHM 对个体数据 $x_i(i=1,2,\cdots,n)$ 进行加密.然后,云服务器可利用加法同态性在密文域上进行数据聚合及各种丰富类型的统计与分析.最后,拥有单向陷门置换 f 对应私钥的授权用户可先由 CA 解密出对称密钥 r,继而进一步解密明文域上聚合运算的结果.与基于同态加密的密文数据聚合相比,不基于同态加密的密文数据聚合不仅无需将公钥加法同态加密作用于每一个个体数据,使得资源受限的移动用户端的效率得到了很大的提高,且符合混合加密的基本原则.

当前国内外学者的主要工作集中在基于云的无线体域网[98-111]、智能电网[112-116]和无线车载网[117-122]的密文数据聚合方面,主要出发点是保护用户的隐私数据.无线体域网中的密钥预分配可以视作隐私保护的数据聚合的准备阶段,多个不同用户之间可先协商共同的会话密钥,为实现多用户时间、空间多维数据隐私保护聚合打下基础.Cherukuri 等人[98]首次在无线体域网中提出基于生物特征的密钥协商协议.2个部署于同一人体不同部位的传感器节点对同一生命体征采集到的数据在一定范围内存在误差.利用 Reed-Solomon 纠错编码技术构造共享密钥机制.随后,Bao 等人[99]利用脉搏间隙(inter-pulse-interval, IPI),基于部署于同一病人不同位置的传感器对同一生命体征采集数据的汉明距离远小于部署于不同病人身体上的传感器对该生命体征采集数据的汉明距离这一观察,构造无线体域网中的会话密钥协商协议.Fuzzy Vault 技术[100]被广泛采用,设计无线体域网中的密钥协商协议.由某一人体传感器节点引入盲化点集合,来混淆从病人人体采集的真实生命体征数据,从而构造 Vault.另一传感器节点能成功与其建立对密钥,当且仅当该 Vault 与其自身对同一生命体征采集到的数据集的交集的大小满足系统预设的门限值.然而,Venkatasubramanian 等人[101]在指出 IPI 信号由于其在不同人体间的低差分性不适宜用作无线体域网对密钥建立的同时,提出了一个基于生理信号 PPG 和 ECG 的认证密钥协商协议.2013 年 Hu 等人[102]基于某些特定的生物特征(如 ECG 信号)是有序排列的且只有采集该信号的传感器才能正确识别该序列这一事实,提出了无线体域网中有序生物特征的密钥协商协议.上述2个方案均利用 Fuzzy Vault 技术实现.

此外,国内外现有工作仅考虑病人身处家庭环境等相对安全的静态场景,然而在现实中,部署无线体域网穿戴设备的病人在进行心电图(ECG)和脑电图(EEG)检查时,可以像普通人群一样在公开环境移动.因此,人体传感器更易遭受包括节点俘获攻击在内的各种攻击,这种新的安全性模型对现有工作提出了极大的挑战.患有同种疾病且隶属于同一社交群体的移动病人可以相互交流病情和诊疗经验[103].Wang 等人[104]提出了一个移动健康网络中的体域网安全模型.Ren 等人[105]提出了一系列在移动医疗社交网络中安全高效的监控病人病情的技术,但并没有给出具体的方案构造.此外,基于 Shamir 秘密共享的主动密钥分发技术,由于在密钥预分配阶段需要为每一个传感器节点分发一个 t 次多项式,在对密钥建立阶段需要进行多项式插值操作,巨大的计算量使其不能直接应用于无线体域网;且未考虑保护病人身份隐私与位置隐私保护问题.最近,我们团队[106]在基于云的移动电子医疗体域网中设计轻量级外包密钥更新算法,提出了能抵抗时间和空间2类移动敌手攻击的,同时保护用户身份隐私、位置隐私及人体传感器部署隐私的密钥管理方案.

为了解决该问题,2014 年我们团队[116]在智能

电网中,提出了一个基于 ElGamal 加密体制的、高效的隐私保护数据聚合方案.该方案只需要额外的产生 2 个密文,就能实现 n 个时间周期内隐私保护的数据聚合功能.因此,其计算开销与时间周期的长度无关.2015 年,我们提出了不依赖于公钥同态加密、利用一次任意单项陷门置换实现的隐私保护数据聚合一般性构造[59].在基于云的车载容斥网络中,利用该一般性新构造,我们提出了安全外包数据包传递证据生成算法,设计了能抵抗夹层合谋攻击这一公开问题的安全数据包传输协议[122].

3.3 存在问题与未来研究方向

本节主要回顾了基于同态加密算法实现的隐私保护密文数据聚合的国内外最新研究进展,并指出现有的通过将公钥同态加密作用于每一个数据来实现隐私保护的方法计算开销大,不能满足大数据环境中资源受限的移动设备的客观需要.并在此基础上重点介绍了在不得不使用公钥加密实现隐私保护的前提下,如何通过尽量减少公钥加密的使用次数,来达到同时对 n 个数据实现隐私保护数据聚合的新技术.然后,现有工作多集中于单用户时间序列密文数据聚合,如何实现高效的多用户隐私保护密文数据聚合,以及各类密文域上的数据统计与分析是一项极富意义的研究课题.

4 结束语

本文主要围绕大数据的安全与隐私保护,指出解决大数据安全与隐私保护最彻底的方法是通过加密来实现.并进一步从密文计算、密文访问控制和密文数据聚合 3 方面对如何在密文域上实现与明文域上相同的大数据技术等国内外研究进展进行综述,并指出其存在问题与不足.尤其重点对我们团队提出的密文计算中不依赖公钥(全)同态加密、且仅需一次离线任意单向陷门置换实现的高效隐私保护外包计算、密文访问控制中支持大属性集合的短密文高效可追踪密文策略属性基加密方案与密文数据聚合中不依赖于加法同态加密的、且能同时保护个体数据隐私与聚合结果隐私的高效隐私保护外包聚合方案,给出了其主要研究思路和研究方法.最后,还针对密文计算、密文访问控制和密文数据聚合 3 方面,指出了当前研究存在的问题和未来的研究方向,以让读者理解各种方法的优劣和适用场景,为进一步从事面向大数据的共享安全理论研究提供了新思路.

参 考 文 献

[1] Cao Zhenfu. New Directions of Modern Cryptography [M] // Boca Raton, FL: CRC Press Inc, 2012

[2] Cao Zhenfu. New development of cryptography [J]. Journal of Sichuan University: Engineering Science Edition, 2015, 47(1): 1-12 (in Chinese)
(曹珍富. 密码学的新发展[J]. 四川大学学报: 工程科学版, 2015, 47(1): 1-12)

[3] Dong Xiaolei. Advances of privacy preservation in Internet of things [J]. Journal of Computer Research and Development, 2015, 52(10): 2341-2352 (in Chinese)
(董晓蕾. 物联网隐私保护研究进展[J]. 计算机研究与发展, 2015, 52(10): 2341-2352)

[4] Cao Zhenfu. New trends of information security—How to change people's life style? [J]. SCIENCE CHINA Information Sciences, 2016, 59(5): 050106

[5] Mayer-Schönberger V, Cukier K. Big data: A Revolution That Will Transform How We Live, Work, and Think [M]. Boston, MA: Houghton Mifflin Harcourt, 2013

[6] Cukier K, Mayer-Schoenberger V. Rise of big data: How it's changing the way we think about the world [J]. The Foreign Affairs, 2013, 92: 28

[7] Feng Dengguo, Zhang Min, Li Hao. Big data security and privacy protection [J]. Journal of Computer, 2014, 37(01): 246-258 (in Chinese)
(冯登国, 张敏, 李昊. 大数据安全与隐私保护[J]. 计算机学报, 2014, 37(1): 246-258)

[8] Lyubashevsky V, Peikert C, Regev O. On ideal lattices and learning with errors over rings [G] //LNCS 6110: Proc of Advances in Cryptology-CRYPTO'10. Berlin: Springer, 2010: 1-23

[9] Halvei S, Gentry C, Vaikuntanathan V. A simple BGN-type cryptosystem from LWE [G] //LNCS 6110: Proc of EUROCRYPT'10. Berlin: Springer, 2010: 506-522

[10] Brakerski Z, Vaikuntanathan V. Fully homomorphic encryption for ringlwe and security for key dependent messages [G] //LNCS 6841: Proc of Advances in Cryptology-CRYPTO'11. Berlin: Springer, 2011: 505-524

[11] Brakerski Z. Fully homomorphic encryption without modulus switching from classical GapSVP [G] //LNCS 7417: Proc of Advances on Cryptology-CRYPTO'12. Berlin: Springer, 2012: 868-886

[12] Brakerski Z, Gentry C, Vaikuntanathan V. Fully homomorphic encryption without bootstrapping [C] // Innovations in Theoretical Computer Science (ITCS). New York: ACM, 2012: 309-325

[13] Gentry C, Halevi S, Smart N. P. Better bootstrapping in fully homomorphic encryption [G] //LNCS 72393: Proc of Public Key Cryptography-PKC'12. Berlin: Springer, 2012: 1-16

[14] Gentry C, Sahai A, Waters B. Homomorphic encryption from learing with errors: comceptually-simpler, asymptotically-faster, attribute-based [G] //LNCS 8042: Proc of Advances in Cryptology—CRYPTO'13. Berlin: Springer, 2013: 75-92

[15] Vercauteren F, Smart N P. Fully homomorphic SIMD operations [J]. Designs, Codes and Cryptography, 2014, 71 (1): 57-81

[16] Lauter K, Naehrig M, Vaikuntanathan V. Can homomorphic encryption be practical? [C] //Proc of ACM CCS 2011. New York: ACM, 2011: 1-12

[17] Gennaro R, Gentry C, Parno B. Non-interactive verifiable computing: Outsourcing computation to untrusted workers [C] //Proc of CRYPTO 2010. Berlin: Springer, 2010, 465-482

[18] Yao A. Protocols for secure computations [C] //Proc of the 23rd Annual Symp on Foundations of Computer Science. Piscataway, NJ: IEEE, 1982: 160-164

[19] Chung K M, Kalai Y, Vadhan S. Improved delegation of computation using fully homomorphic encryption [C] //Proc of CRYPTO 2010. Berlin: Springer, 2010: 483-501

[20] Applebaum B, Ishai Y, Kushilevitz E. From secrecy to soundness: Efficient verification via secure computation [C] //Proc of the 37th Int Colloquium in Automata, Languages and Programming. Berlin: Springer, 2010: 152-163

[21] Benabbas S, Gennaro R, Vahlis Y. Verifiable delegation of computation over large datasets [C] //Proc of the 31st Annual Conf on Advances in Cryptology. Berlin: Springer, 2011: 111-131

[22] Barbosa M, Farshim P. Delegatable homomorphic encryption with applications to secure outsourcing of computation [C] // Proc of CT-RSA 2012. Berlin: springer, 2012: 296-312

[23] Fiore D, Gennaro R, Pastro V. Efficiently verifiable computation on encrypted data [C] //Proc of the 2014 ACM Conf on Computer and Communications Security. New York: ACM, 2014: 844-855

[24] Parno B, Raykova M, Vaikuntanathan V. How to delegate and verify in public: verifiable computation from attribute based encryption [C] //Proc of Theory of Cryptography. Berlin: Springer, 2012: 422-439

[25] Fiore D, Gennaro R. Publicly verifiable delegation of large polynomials and matrix computations, with applications [C] //Proc of the 2012 ACM Conf on Computer and Communications Security. New York: ACM, 2012: 501-512

[26] Catalano D, Fiore D, Gennaro D, et al. Algebraic (trapdoor) one-way functions and their applications [C] // Proc of Theory of Cryptography. Berlin: Springer, 2013: 680-699

[27] Papamanthou C, Shi E, Tamassia R. Signatures of correct computation [C] //Proc of Theory of Cryptography. Berlin: Springer, 2013: 222-242

[28] Choi S G, Katz J, Kumaresan R, et al. Multi-client non-interactive verifiable computation [C] //Proc of Theory of Cryptography. Berlin: Springer, 2013: 499-518

[29] Goldwasser S, Goyal V, Jain A, et al. Multi-input function encryption [C] //Proc of EUROCRYPT 2014. Berlin: Springer, 2014: 578-602

[30] Gordon S D, Katz J, Liu F H, et al. Multi-client verifiable computation with stronger security guarantees [C] //Proc of Theory of Cryptography Conf. Berlin: Springer, 2015: 144-168

[31] Rivest R, Shamir A, Adleman L. On data banks and privacy homomorphisms [J]. Foundations of Secure Computation, Georgia Institute of Technology, 1978, 21(2): 169-180

[32] Rivest R, Shamir A, Adleman L. A methord for obtaining digital signatures and public key cryptosystems [J]. Communications of the ACM, 1978, 21(2): 120-126

[33] ElGamal T. A public key cryptosystem and a signature scheme based on discrete logarithms [J]. IEEE Trans on Information Theory, 1985, 31(4): 469-472

[34] Goldwasser S, Micali S. Probabilistic encryption [J]. Journal of Computer and Systems Sciences, 1984, 28(2): 270-299

[35] Benaloh J. Dense probabilistic encryption [C] //Proc of the Workshop on Selected Areas of Cryptography. Berlin: Springer, 1994: 120-128

[36] Naccache D, Stern J. A new public key cryptosystem based on higher residues [C] //Proc of the 5th ACM Conf on Computer and Communications Security. New York: ACM, 1998: 59-66

[37] Okamoto T, Uchiyama S. A new public-key cryptosystem as secure as factoring [G] //LNCS 1403: Proc of Advances in Cryptology—EUROCRYPT'98. Berlin: Springer, 1998: 308-318

[38] Paillier P. Public-key cryptosystems based on composite degree residuosity classes [G] //LNCS 1592: Proc of Advances in Cryptology—EURCRYPT'99. Berlin: Springer, 1999: 223-238

[39] Boneh D, Goh E J, Nissim K. Evaluation 2-dnf fomulas on ciphertexts [G] //LNCS 3378: Theory of Cryptoography. Berlin: Springer, 2005: 325-341

[40] Gentry C. Fully homomorphic encryption using ideal lattices [C] //Proc of the 41st ACM Symp on Theory of Computing (STOC). New York: ACM, 2009: 169-178

[41] Smart N P, Vercauteren F. Fully homomorphic encryption with relatively small key and ciphertext size [G] //LNCS 6056: Proc of PKC 2010. Berlin: Springer, 2010: 420-443

[42] Stehle D, Steinfeld R. Faster fully homomorphic encryption [G] //LNCS 6477: Proc of Advances in Cryptology—ASIACRYPT'10. Berlin: Springer, 2010: 377-394

[43] Gentry C, Halevi S. Implementing gentry's fully-homomorphic encryption scheme [G] //LNCS 6632: Proc of Advances in Cryptology—EUROCRYPT'11. Berlin: Springer, 2011: 129-148

[44] Dijk M, Gentry C, Halevi S, et al. Fully homomorphic encryption over the integers [G] //LNCS 6110: Proc of Advances in Cryptology—EURCRYPT'10. Berlin: Springer, 2010: 24-43

[45] Damgård I, Polychroniadou A, Rao V. Adaptively secure multi-party computation from lwe (via equivocal fhe)[C] // Proc of IACR Int Workshop on Public Key Cryptography. Berlin: Springer, 2016: 208-233

[46] Gordon S D, Katz J, Liu F H, et al. Multi-client verifiable computation with stronger security guarantees [C] //Proc of Theory of Cryptography Conf. Berlin: Springer, 2015: 144-168

[47] Wang C, Ren K, Wang J. Secure optimization computation outsourcing in cloud computing: A case study of linear programming [J]. IEEE Trans on Computers, 2016, 65(1): 216-229

[48] Chen X, Huang X, Li J, et al. New algorithms for secure outsourcing of large-scale systems of linear equations [J]. IEEE Trans on Information Forensics and Security, 2015, 10 (1): 69-78

[49] Alderman J, Janson C, Cid C, et al. Hybrid publicly verifiable computation [C] //Proc of Cryptographers' Track at the RSA Conf. Berlin: Springer, 2016: 147-163

[50] Zhou Jun, Dong Xiaolei, Cao Zhenfu. Advances of Ciphertext access control and privacy preserving [J]. Bulletin of Chinese Association for Cryptologic Research, 2015, 41 (6): 19-21 (in Chinese)
(周俊, 董晓蕾, 曹珍富. 密文访问控制与隐私保护研究进展 [J]. 中国密码学会通讯, 2015, 41(6): 19-21)

[51] Brakerski Z, Vaikuntanathan V. Efficient fully homomorphic encryption from (standard) LWE [C] //Proc of FOCS. Los Alamitos. CA: IEEE Computer Society, 2011: 97-106

[52] Brakerski Z, Gentry C, Vaikuntanathan V. (Leveled) fully homomorphic encryption without bootstrapping [C] //Proc of ITCS. New York: ACM, 2012, 309-325

[53] Halevi S, Shoup V. Algorithm in HElib [G] //LNCS 8616: Proc of CRYPTO 2014 Part I. Berlin: Springer, 2014: 554-571

[54] Dowlin N, Gilad-Bachrach R, Laine K, et al. Manual for using for homomorphic encryption for bioinformatics, MSR-TR-2015-87 [R]. New York: Microsoft Research, 2015

[55] Gentry C, Halevi S, Smart N P. Homomorphic evaluation of the AES circuit [C] //Proc of Advances in Cryptology—CRYPTO 2012. Berlin: Springer, 2012: 850-867

[56] Cheon J H, Lee H T, Seo J H. A new additive homomorphic encryption based on the co-ACD problem [C] //Proc of ACM CCS 2014. New York: ACM, 2014: 287-298

[57] Costache A, Smart N P, Vivek S, et al. Fixed point arithmetic in SHE scheme [J]. ePrint 2016/250, 2016

[58] Cheon J H, Kim A, Kim M, et al. Floating-point homomorphic encryption [J]. ePrint 2016/421, 2016

[59] Zhou Jun, Cao Zhenfu, Dong Xiaolei, et al. Security and privacy in cloud-assistedwireless wearable communications: challenges, solutions and future directions [J]. IEEE Wireless Communications, 2015, 22(2): 136-144

[60] Zhou Jun, Cao Zhenfu, Dong Xiaolei, et al. EVOC: More efficient verifiable outsourced computation from any one-way trapdoor function [C] //Proc of IEEE ICC 2015. Piscataway, NJ: IEEE, 2015: 7444-7449

[61] Zhou Jun, Cao Zhenfu, Dong Xiaolei. PPOPM: More efficient privacy preserving outsourced pattern matching [C] //Proc of ESORICS 2016. Berlin: Springer, 2016: 135-153

[62] Zhou Jun, Cao Zhenfu, Dong Xiaolei, et al. PPDM: A privacy-preserving protocol forcloud-assisted e-healthcare systems [J]. IEEE Journal of Selected Topics in SignalProcessing, 2015, 9(7): 1332-1344

[63] Sahai A, Waters B. Fuzzy Identity-Based Encryption [C] // Proc of EUROCRYPT 2005. Berlin: Springer, 2005: 457-473

[64] Cheung L, Newport C C. Provably secure ciphertext policy ABE [C] //Proc of 2007 ACM Conf on Computer and Communications Security (CCS). New York: ACM, 2007: 456-465

[65] Goyal V, Jain A, Pandey O, et al. Bounded ciphertext policy attribute based encryption [C] //Proc of the Int Colloquium on Automata, Languages, and Programming. Berlin: Springe, 2008: 579-591

[66] Emura K, Miyaji A, Nomura A, et al. A ciphertext-policy attribute-based encryption scheme with constant ciphertext length [C] //Proc of the Int Conf on Information Security Practice and Experience. Berlin: Springer, 2009: 13-23

[67] Herranz J, Laguillaumie F, Ràfols C. Constant size ciphertexts in threshold attribute-based encryption [C] //Proc of the Int Workshop on Public Key Cryptography. Berlin: Springer, 2010: 19-34

[68] Lewko A, Waters B. Unbounded HIBE and attribute-based encryption [C] //Proc of the Annual Int Conf on the Theory and Applications of Cryptographic Techniques. Berlin: Springer, 2011: 547-567

[69] Okamoto T, Takashima K. Fully secure unbounded inner-product and attribute-based encryption [C] //Proc of the Int Conf on the Theory and Application of Cryptology and Information Security. Berlin: Springer, 2012: 349-366

[70] Rouselakis Y, Waters B. Practical constructions and new proof methods for large universe attribute-based encryption [C] //Proc of ACM CCS 2013. New York: ACM, 2013: 463-474

[71] Green M, Hohenberger S, Waters B. Outsourcing the decryption of ABE ciphertexts [C/OL] //Proc of USENIX Security Symp. Berkeley, CA : USENIX, 2011 [2016-06-15]. http://citeseerx. ist. psu. edu/viewdoc/download? doi = 10. 1. 1. 306. 9655&rep=rep1&type=pdf

[72] Lewko A, Waters B. New proof methods for attribute-based encryption: Achieving full security through selective techniques [C] //Proc of the Advances in Cryptology—CRYPTO 2012. Berlin: Springer, 2012: 180-198

[73] Hohenberger S, Waters B. Attribute-based encryption with fast decryption [C] //Proc of Public-Key Cryptography—PKC 2013. Berlin : Springer, 2013: 162-179

[74] Hohenberger S, Waters B. Online/offline attribute-based encryption [C] //Proc of the Int Workshop on Public Key Cryptography. Berlin: Springer, 2014: 293-310

[75] Boneh D, Gentry C, Gorbunov S, et al. Fully key-homomorphic encryption, arithmetic circuit ABE and compact garbled circuits [C] //Proc of the Annual Int Conf on the Theory and Applications of Cryptographic Techniques. Berlin: Springer, 2014: 533-556

[76] Yamada S, Attrapadung N, Hanaoka G, et al. A framework and compact constructions for non-monotonic attribute-based encryption [C] //Proc of the Int Workshop on Public Key Cryptography. Berlin: Springer, 2014: 275-292

[77] Kowalczyk L, Lewko A B. Bilinear entropy expansion from the decisional linear assumption [C] //Proc of Advances in Cryptology—CRYPTO 2015. Berlin: Springer, 2015: 524-541

[78] Chen J, Gay R, Wee H. Improved dual system ABE in prime-order groups via predicate encodings [C] //Proc of Advances in Cryptology—EUROCRYPT 2015. Berlin: Springer, 2015: 595-624

[79] Gorbunov S, Vinayagamurthy D. Riding on asymmetry: Efficient ABE for branching programs [C] //Proc of Advances in Cryptology—ASIACRYPT 2015. Berlin: Springer, 2015: 550-574

[80] Attrapadung N, Hanaoka G, Yamada S. Conversions among several classes of predicate encryption and applications to abe with various compactness tradeoffs [C] //Proc of Advances in Cryptology—ASIACRYPT 2015. Berlin: Springer, 2015: 575-601

[81] Brakerski Z, Vaikuntanathan V. Circuit-ABE from LWE: Unbounded attributes and semi-adaptive security [J]. IACR Cryptology ePrint Archive, 2016

[82] Gong Junqing, Cao Zhenfu, Tang S, et al. Extended dual system group and shorter unbounded hierarchical identity based encryption [J]. Designs, Codes and Cryptography, 2016, 80(3), 525-559

[83] Gong Junqing, Chen Jun, Dong Xiaolei, et al. Extended nested dual system groups, revisited [C] //Proc of PKC 2016. Berlin: Springer, 2016: 133-163

[84] Attrapadung N, Hanaoka G, Yamada S. A framework for identity-based encryption with almost tight security [C] // Proc of the Int Conf on the Theory and Application of Cryptology and Information Security. Berlin: Springer, 2015: 521-549

[85] Jason H, Jiang S, Safavi-Naini R, et al. Attribute-based encryption with key cloning protection [J]. IACR Cryptology ePrint Archive 2008, 2008: No. 478

[86] Yu S, Ren K, Lou W, et al. Defending against key abuse attacks in KP-ABE enabled broadcast systems [C] //Proc of the Int Conf on Security and Privacy in Communication Systems. Berlin: Springer, 2009: 311-329

[87] Katz J, Schroder D. Tracing insider attacks in the context of predicate encryption schemes [J/OL]. ACITA 2011. [2016-06-15]. https://www.usukita.org/node/1779

[88] Liu Zhen, Cao Zhenfu, Wong D S. White-box traceable ciphertext-policy attribute-based encryption supporting any monotone access structures [J]. IEEE Trans on Information Forensics and Security, 2013, 8(1): 76-88

[89] Ning Jianting, Cao Zhenfu, Dong Xiaolei, et al. Traceable CP-ABE with short ciphertexts: How to catch people selling decryption devices on eBay efficiently [C] //Proc of the European Symp on Research in Computer Security. Berlin: Springer, 2016: 551-569

[90] Liu Zhen, Cao Zhenfu, Wong D S, Blackbox traceable CP-ABE: How to catch people leaking their keys by selling decryption devices on ebay [C] //Proc of ACM Conf on Computer and Communications Security. New York: ACM, 2013: 475-486

[91] Ning Jianting, Cao Zhenfu, Dong Xiaolei, et al. Large universe ciphertext-policy attribute-based encryption with white-box traceability [C] //Proc of the European Symp on Research in Computer Security. Berlin: Springer, 2014: 55-72

[92] Ning Jianting, Cao Zhenfu, Dong Xiaolei, et al. White-box traceable ciphertext-policy attribute-based encryption supporting flexible attributes [J]. IEEE Trans on Information Forensics and Security (TIFS), 2015, 10(6): 1274-1288

[93] Ning Jianting, Cao Zhenfu, Dong Xiaolei, et al. Accountable authority ciphertext-policy attribute-based encryption with white-box traceability and public auditing in the cloud [C] // Proc of the European Symp on Research in Computer Security. Berlin: Springer, 2015: 270-289

[94] Hur J, Noh D K, Attribute-based access control with efficient revocation in data outsourcing systems [J]. IEEE Trans on Parallel Distribute System, 2011, 22(7): 1214-1221

[95] Liang Xiaohui, Cao Zhenfu, Lin Huang, et al. Attribute based proxy re-encryption with delegating capabilities [C] // Proc of the 4th Int Symp on Information, Computer, and Communications Security. New York: ACM, 2009: 276-286

[96] Qian Junlei, Dong Xiaolei. Fully secure revocable attribute-based encryption [J]. Journal of Shanghai Jiaotong University (Natural Science Edition), 2011, 16(4): 490-496

[97] Sahai A, Seyalioglu H, Waters B. Dynamic credentials and ciphertext delegation for attribute-based encryption [C] // Proc of the Advances in Cryptology—CRYPTO 2012. Berlin: Springer, 2012: 199-217

[98] Cherukuri S, Venkatasubramanian K K, Gupta S K S. BioSec: A biometric based approach for securing communication in wireless networks of biosensors implanted in the human body [C] //Proc of IEEE Int Conf on Parallel Processing Workshop. Piscataway, NJ: IEEE, 2003: 432-439

[99] Bao S D, Poon C C Y, Zhang Y T, et al. Using the timing information of hearbeats as an entity identifier to secure body sensor network [J]. IEEE Trans on Information Technology in Biomedicine, 2008, 12(6): 772-779

[100] Juels A, Sudan M. A fuzzy vault scheme [J]. Designs, Codes and Cryptography, 2006, 38(2): 237-257

[101] Venkatasubramanian K K, Banerjee A, Gupta S K S. PSKA: Usable and secure key agreement scheme for body area networks [J]. IEEE Trans on Information Technology in Biomedicine, 2010, 14(1): 60-68

[102] Hu C, Cheng X, Zhang F, et al. OPFKA: Secure and efficient ordered-physiological-feature-based key agreement for wireless body area networks [C] //Proc of INFOCOM 2013. Piscataway, NJ: IEEE, 2013: 2274-2282

[103] Lu R, Lin X, Liang X, et al. A secure handshake scheme with symptoms-matching for mhealthcare social network [J]. Mobile Networks and Applications, 2011, 16(6): 683-694

[104] Wang H, Fang H, Xing L, et al. An integrated biometric-based security framework using wavelet-domain HMM in wireless body area networks (WBAN) [C] //Proc of the 2011 IEEE Int Conf on Communications (ICC). Piscataway, NJ: IEEE, 2011: 1-5

[105] Ren Y, Werner R, Pazzi N, et al. Monitoring patients via a secure and mobile healthcare system [J]. IEEE Wireless Communications, 2010, 17(1): 59-65

[106] Zhou Jun, Cao Zhenfu, Dong Xiaolei, et al. 4S: A secure and privacy-preserving key management scheme for cloud-assisted wireless body area network in m-healthcare social networks [J]. Information Sciences, 2015, 314: 255-276

[107] Zhang R, Zhang Y, Sun J, et al. Fine-grained private matching for proximity-based mobile social networking [C] //Proc of INFOCOM 2012. Piscataway, NJ: IEEE, 2012: 1969-1977

[108] Liang X, Li X, Zhang K, et al. Fully anonymous profile matching in mobile social networks [J]. IEEE Journal on Selected Areas of Communications (JSAC), 2013, 31(9): 641-655

[109] Li L, Zhao X, Xue G, et al. Privacy preserving group ranking [C] //Proc of the 32nd Int Conf on Distributed Computing Systems (ICDCS). Piscataway, NJ: IEEE, 2012: 214-223

[110] Zhang L, Li X Y, Liu Y, et al. Verifiable private multi-party computation: Ranging and ranking [C] //Proc of INFOCOM 2013. Piscataway, NJ: IEEE, 2013: 605-609

[111] Li X Y, Jung T. Search me if you can: Privacy-preserving location query service [C] //Proc of INFOCOM 2013. Piscataway, NJ: IEEE, 2013: 2760-2768

[112] Lu R, Liang X, Li X, et al. EPPA: An efficient and privacy-preserving aggregation scheme for secure smart grid communications [J]. IEEE Trans on Parallel and Distributed Systems, 2012, 23(9): 1621-1631

[113] Erkin Z, Tsudik G. Private computation of spatial and temporal power consumption with smart meters [G] // LNCS 7341: Proc of ACNS'12. Berlin: Springer, 2012: 561-577

[114] Liang X, Li X, Lu R, et al. UDP: Usage based dynamic pricing with privacy preservation for smart grid [J]. IEEE Trans on Smart Grid, 2013, 4(1): 141-150

[115] Won J, Ma C Y T, Yau D K Y, et al. Proactive fault-tolerant aggregation protocol for privacy-assured smart metering [C] //Proc of the IEEE Conf on Computer Communications (INFOCOM 2014). Piscataway, NJ: IEEE, 2014: 2804-2812

[116] Dong Xiaolei, Zhou J, Alharbi K, et al. An ElGamal-based efficient and privacy-preserving data aggregation scheme for smart grid [C] //Proc of IEEE Globecom 2014. Piscataway, NJ: IEEE, 2014: 4720-4725

[117] Lin X, Sun X, Wang X, et al. TSVC: Timed efficient and secure vehicular communications with privacy preserving [J]. IEEE Trans on Wireless Communication, 2008, 12(7): 4987-4998

[118] Zhang C, Lin X, Lu R, et al. RAISE: An efficient RSU-aided message authentication scheme in vehicular communication networks [C] //Proc of IEEE ICC. Piscataway, NJ: IEEE, 1451-1457

[119] Lin X, Li X. Achieving efficient cooperative message authentication in vehicular ad hoc networks [J]. IEEE Trans on Vehicular Technology, 2013, 62(7): 3339-3348

[120] Lu R, Lin X, Liang X, et al. A dynamic privacy-preserving key management scheme for location based services in VANETs [J]. IEEE Trans on Intelligent Transportation Systems, 2012, 13(1): 127-139

[121] Lu R, Lin X, Luan T H, et al. PReFilter: An efficient privacy-preserving relay filtering scheme for delay tolerant networks [C] //Proc IEEE INFOCOM'12. Piscataway, NJ: IEEE, 1395-1403

[122] Zhou Jun, Dong Xiaolei, Cao Zhenfu, et al. Secure and privacy preserving protocol for cloud-based vehicular DTNs [J]. IEEE Trans on Information Forensics and Security, 2015, 10(6): 1299-1314

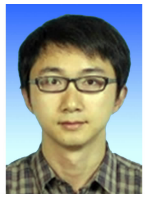
[123] Liang Xiaohui, Cao Zhenfu, Lin Huang, et al. Attribute based proxy re-encryption with delegating capabilities [C] // Proc of ASIACCS 2009. New York: ACM, 2009: 276-286

[124] Liu Zhen, Cao Zhenfu, Huang Qiong, et al. Fully secure multi-authority ciphertext-policy attribute-based encryption without random oracles [G] //LNCS 6879: Proc of European Symp on Research in Computer Security (ESORICS 2011). Berlin: Springer, 2011: 278-297

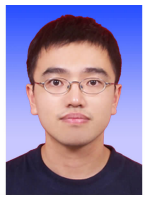
[125] Zhou Jun, Cao Zhenfu, Dong Xiaolei, et al. TR-MABE: White-box traceable and revocable multi-authority attribute-based encryption and its applications to multi-level privacy-preserving e-healthcare cloud computing systems [C] //Proc of IEEE INFOCOM 2015. Piscataway, NJ: IEEE, 2015: 2398-2406

Cao Zhenfu, born in 1962. PhD, distinguished professor in East China Normal University. His main research interests include number theory and new theories for cryptography and network security (security and privacy preserving for cloud computing and big data processing).

Dong Xiaolei, born in 1971. PhD, distinguished professor in East China Normal University. Her main research interests include number theory, cryptography and network security, and big data security and privacy preserving (dongxiaolei@sei.ecnu.edu.cn).



Zhou Jun, born in 1982. PhD, Chen Hui Scholar in East China Normal University. His main research interests include key theories for secure outsourced computation and privacy preserving, and the applied cryptography in big data processing (jzhou@sei.ecnu.edu.cn).



Shen Jiachen, born in 1979. PhD, lecturer in East China Normal University. His main research interests include searchable encryption and signal processing in the encrypted domain (jcshen@sei.ecnu.edu.cn).

Ning Jianting, born in 1988. PhD candidate in Shanghai Jiao Tong University. His main research interests include attribute-based encryption, identity-based encryption, functional encryption, zero knowledge proof, and applications in cloud computing and big data (jelly408385909@163.com).

Gong Junqing, born in 1986. PhD candidate in Shanghai Jiao Tong University. His main research interests include construction and analysis for functional encryption (gongjunqing@126.com).